

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-182244

(43)Date of publication of application : 21.07.1995

(51)Int.Cl.

G06F 12/14
G09C 1/00

(21)Application number : 05-322872

(71)Applicant : RICOH CO LTD

(22)Date of filing : 21.12.1993

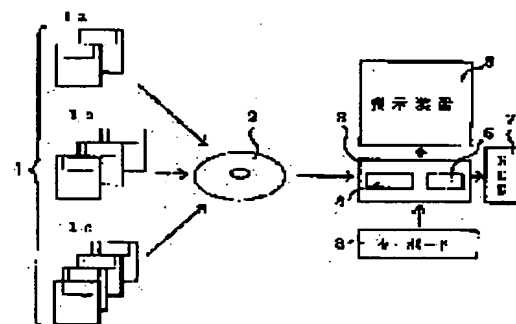
(72)Inventor : MOTOHASHI HIROOMI

(54) METHOD FOR DISTRIBUTING SOFTWARE

(57)Abstract:

PURPOSE: To prevent distributed software(SW) from being illicitly used and to know an outflow route of the SW even when the SW is illicitly used in an SW distributing method for ciphering plural SW, storing the ciphered SW in a recording medium and then distributing the stored SW.

CONSTITUTION: A user identifying information storing area for individually storing information for identifying each user is previously prepared and plural software to be ciphered and distributed are stored in a CD-ROM 2 being a recording medium and then distributed. A pass-word obtained by synthesizing a decoding key for each software and user identifying information and ciphering the synthesized result is given only to a user allowed to use anyone of the SW, and when the CD-ROM 2 is loaded to a personal computer 3 and the pass- word is inputted, a decoding program 6 is started and the SW corresponding to the decoding key is decided and the user identifying information separated from the pass-word is written in a user identifying information storing area for the decoded SW.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

Japanese Publication for Unexamined Patent Application
No. 182244/1995 (Tokukaihei 7-182244)

A. Relevance of the Above-identified Document

This document has relevance to Claims 1, 5, 9 and 15 of the present application.

B. Translation of the Relevant Passages of the Document

[0004] ...a software supplier stores a plurality of software programs in a CD-ROM by encoding them but not encoding those for demonstration, so as to distribute the CD-ROM to users either free of charge or at a reasonable rate. The users who received the distributed CD-ROM try out the software programs for demonstration, then, if any of them is desired, purchase an decoder key (password) for the desired software program, thereby using the decoded software program.

[0005]

[PROBLEMS TO BE SOLVED BY THE INVENTION] However, the above distribution method has problems such that it is impossible to (i) detect an illegal password leaking route through which a user who does not pay properly learns a password from a user who properly paid for the password, and illegally restores software, and (ii) prevent illegal copies of software from being produced

THIS PAGE BLANK (USPTO)

based on the original software which was legally restored by a user.

[0013] These software programs 1a, 1b and 1c are previously given regions for storing information to identify a user ...

[0014] Thus prepared software programs are encoded and stored in a CD-ROM 2 so as to be distributed.

[0015] ...a user who received a CD-ROM, if he or she desires any of the software programs in the CD-ROM, advises a software supplier who distributed the software program of his/her address, full name, the model and serial number of a computer to be used to execute the software program, etc., then, obtains a decoder password from the supplier by, for example, paying and/or obtaining a license to use the software program.

[0016] Once obtaining a password for the desired software program, the software program is restored using a decoder program and a password.

[0017] ... A decoder program 6 separates the user's full name as user identification information and a decoder key from the readout password, and examines whether or not the decoder key is legal. In the case of the legal decoder key, software is decoded with the decoder key, then, the user's full name being the user

THIS PAGE BLANK (USPTO)

identification information is written into a user identification information storing region in the decoded software, thereafter writing the software into a hard disk device (HDD) 7.

[0020] ...the user's full name is utilized so as to simplify explanation. However, the user's registration number (the number for management given by the software supplier when the user requests a license for use), or address and full name may be used instead. When the user is a juridical person, illegal copies of the software can be prevented within a corporation by previously storing the appellation of the corporation and a belonging group.

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平7-182244

(43)公開日 平成7年(1995)7月21日

(51)Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0 E			
	B			
G 0 9 C 1/00	3 1 0	9364-5L		

審査請求 未請求 請求項の数3 O L (全 5 頁)

(21)出願番号 特願平5-322872

(22)出願日 平成5年(1993)12月21日

(71)出願人 000006747

株式会社リコー

東京都大田区中馬込1丁目3番6号

(72)発明者 本橋 弘臣

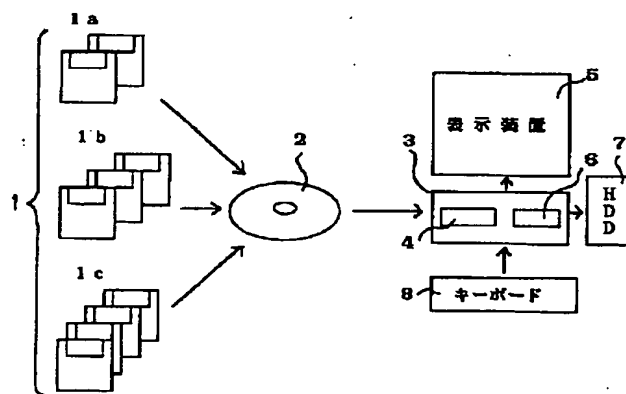
東京都大田区中馬込1丁目3番6号 株式会社リコー内

(54)【発明の名称】 ソフトウェア配布方法

(57)【要約】

【目的】 複数のソフトウェアを暗号化して記憶媒体に格納して配布するソフトウェアの配布方法において、配布したソフトウェアの不正な使用を防止し、万一不正使用された場合にもその流出経路を知ることができるようにする。

【構成】 暗号化して配布する複数のソフトウェアを個々に利用者を識別するための情報を格納する利用者識別情報格納領域を予め設けて記憶媒体であるCD-ROM2に格納して配布する。そして、いずれかのソフトウェアの利用を許可した者に対してのみ個々のソフトウェアの復号化キーと利用者識別情報とを合成して暗号化したパスワードを与え、CD-ROM2がパソコン3にセットされてそのパスワードが入力されたとき、復号プログラム6が起動して復号化キーに対応するソフトウェアを復号するとともに、復号したソフトウェアの利用者識別情報格納領域にパスワードから分離した利用者識別情報を書き込む。



(2)

【特許請求の範囲】

【請求項1】記憶媒体に複数のコンピュータプログラムやデータ等のソフトウェアを暗号化して格納し配布する方法において、配布する複数のソフトウェアには個々に利用者を識別するための情報を格納する利用者識別情報格納領域を予め設けておき、そのいずれかのソフトウェアの利用を許可した者にのみ個々のソフトウェアの復号化キーと利用者識別情報とを合成して暗号化したパスワードを与え、そのパスワードの入力により復号プログラムを起動させ、前記複数のソフトウェアのうちの復号化キーに対応するソフトウェアを復号するとともに、入力されたパスワードから利用者識別情報を分離して、その利用者識別情報を復号したソフトウェアの利用者識別情報格納領域に書き込むことを特徴とするソフトウェア配布方法。

【請求項2】前記復号プログラムを、暗号化した複数のコンピュータプログラムやデータ等のソフトウェアとともに前記記憶媒体に格納することを特徴とする請求項1記載のソフトウェア配布方法。

【請求項3】請求項1又は2記載のソフトウェア配布方法において、コンピュータプログラムのソフトウェアには前記利用者識別情報格納領域に格納されている利用者識別情報を可視化または音声化して出力するための命令を含ませることを特徴とするソフトウェア配布方法。

【発明の詳細な説明】**【0001】**

【産業上の利用分野】この発明はソフトウェア配布方法に関し、より詳しくは暗号化して記憶媒体に格納して配布するソフトウェアの不正使用を防止するための方法に関するものである。

【0002】

【従来の技術】パーソナルコンピュータやワークステーションのソフトウェアは3.5インチや5インチのフロッピーディスク等に格納されて配布されることが多い。この場合、通常は文書作成ソフトウェアやデータベースソフトウェアの様に1つのまとまった業務に使用するソフトウェアを1枚もしくは数枚のフロッピーディスクに格納し配布していた。この様な形態での配布では不法コピー（不法複写）を防止するため、プロテクトと称して通常のオペレーティングシステムのコマンドでは複写できないようにフロッピーディスク中に不良セクターを故意に混在させたり、特殊なフォーマットを施していた。

【0003】近年、光ディスクの普及はめざましく、特にCD-ROMは先行したコンパクトディスク（CD-AUDIO）の流行にともない、CD-ROMを読みだす装置（CD-ROMドライブ）も安価に入手できるようになった。そしてパーソナルコンピュータやワークステーションにもCD-ROMドライブが接続され、大容量記憶装置として使用されるようになってきている。ソ

フトウェアの配布方法もこのCD-ROMの持つ大容量（フロッピーディスクの400から500枚分の容量）、小型、薄型、軽量、作成が安価という特徴を活かし、上記文書作成ソフトウェアやデータベースソフトウェアなど従来の配布単位を複数分まとめて個々に暗号化してCD-ROMに格納し、配布する方法が行われるようになった（例えば日経エレクトロニクス 1993年9月13日号参照）。

【0004】上記の配布方法によれば、ソフトウェアの供給者は、CD-ROMに複数のソフトウェアを暗号化し、またデモンストレーション用のソフトウェアを暗号化せずにCD-ROMに格納して利用者に無料若しくは低価格で配布する。配布を受けた利用者はデモンストレーション用のソフトウェアを実行して所望とするソフトウェアがあったら料金と引換に当該ソフトウェアの復号化キー（パスワード）を受け取り、ソフトウェアを復元して使用するようになっていく。このように1つの媒体に多数のソフトウェアを格納して、しかも安価に配布できるのでソフトウェアの流通コストを大幅に削減できるという効果がある。

【0005】

【発明が解決しようとする課題】しかしながら、上記の配布方法では正当な料金を支払っていない利用者が、料金を支払った正当な利用者からパスワードを聞いたりして、不正な手段でソフトウェアを復元してもパスワードの流出経路を知る方法がなく、また正当な利用者が復元したソフトウェアを複製したりする不法コピーを防止できなかった。

【0006】この発明は上記のような問題点を解決するためになされたものであり、配布したソフトウェアの不正な使用を防止し、万一不正使用された場合にもその流出経路を知ることができるようにすることを目的とする。

【0007】なお、この明細書でいうソフトウェアはコンピュータ（マイクロコンピュータも含む）への一連の命令が記録されたコンピュータプログラム（以降単にプログラムと呼ぶ）だけでなく、取り扱い説明書等の文書データやデータベース、フォント、画面に表示すべきグラフィックスやイメージのデータ、音声に変換されるべきデータ等（以降単にデータと呼ぶ）も含めてソフトウェアと呼ぶ。

【0008】

【課題を解決するための手段】上記の目的を達成するため、この発明は記憶媒体に複数のプログラムやデータ等のソフトウェアを暗号化して格納し配布する方法において、配布する複数のソフトウェアには個々に利用者を識別するための情報を格納する利用者識別情報格納領域を予め設けておき、そのいずれかのソフトウェアの利用を許可した者にのみ個々のソフトウェアの復号化キーと利用者識別情報とを合成して暗号化したパスワードを与

(3)

え、そのパスワードの入力により復号プログラムを起動させ、前記複数のソフトウェアのうちの復号化キーに対応するソフトウェアを復号するとともに、入力されたパスワードから利用者識別情報を分離して、その利用者識別情報を復号したソフトウェアの利用者識別情報格納領域に書き込むように構成した。

【0009】また、前記復号プログラムを、暗号化した複数のコンピュータプログラムやデータ等のソフトウェアとともに前記記憶媒体に格納するようにしている。

【0010】さらに、コンピュータプログラムのソフトウェアには前記利用者識別情報格納領域に格納されている利用者識別情報を可視化または音声化して出力するための命令を含ませるように構成した。

【0011】

【作用】この発明によるソフトウェア配布方法では、配布すべき各ソフトウェアは利用者を識別する情報を格納するための領域を確保して暗号化される。そして、そのソフトウェアの利用を許可する者に与えるパスワードの入力により、復号プログラムが起動してパスワード中の復号化キーに対応するソフトウェアを復号したとき、そのパスワードから分離した利用者識別情報を復号したソフトウェアの利用者識別情報格納領域に書き込むので、復号されたソフトウェアがプログラムの場合にはその実行時に格納されている利用者識別情報を出力したり、復号されたソフトウェアがデータの場合でも、そのデータを参照するプログラムがそこに格納されている利用者識別情報を出力することが可能になる。

【0012】

【実施例】以下、図を参照してこの発明の実施例の詳細を説明する。図1はこの発明の一実施例を示すソフトウェアの配布方法を模式的に示したものである。この図で、1は供給すべきソフトウェアで、プログラムもあれば取り扱いを説明する文書もあり、プログラムであっても利用者が直接起動しないデバイスドライバであってもよく、またデータベースのデータやイメージ、音声データでもよい。1a、1b、1cは従来ではそれぞれ販売や配布の単位となっていたソフトウェアである。

【0013】これらのソフトウェア1a、1b、1cには利用者を識別する情報を格納するための領域を予め確保しておき、更にこれらのソフトウェア1a、1b、1cのうちプログラムであるものには、実行の開始時点等上記の格納領域中の情報を出力する命令も予め他の命令に含めておく。上記の具体的な方法は、データなら先頭や末尾に空白のデータ領域を設けておけばよいし、プログラムなら出力命令が参照するアドレス領域を予め空白にしておき、デバッガやダンププログラムのようなソフトウェアツールを利用して実行モジュールになってハードディスク等に格納されたときのファイル中の位置を確かめればよい。そして復号プログラムにはこのファイル中の位置を格納しておけばよい。

【0014】このように用意したソフトウェアを暗号化してCD-ROM2へ格納して配布する。なおCD-ROM2には以上述べたソフトウェアの他に必要に応じて、機密の保護や料金の徴収を要しないデモンストラーションのソフトウェアや試用版のソフトウェアを暗号化しないで格納してもよい。暗号化の方法については各種の先行技術が知られており、ここでは説明を省略する。また暗号化する前に圧縮操作を施したり、アーカイブ（1つのファイルにまとめたりする操作）を施すとCD-ROM2上の領域を節約できたり、復号のための操作を簡略化できる。これら圧縮もアーカイブも公知の技術なので説明は省略する。

【0015】一方、CD-ROMを受け取った利用者はCD-ROM中に所望のソフトウェアがあったら、そのソフトウェアの供給者へ住所、氏名、稼働対象コンピュータの機種、シリアルナンバー等を告げ、料金を支払うなり、ソフトウェアの使用の許諾を受け、供給者より復号のためのパスワードを得る。ここでは説明のため利用者識別情報として氏名を用い暗号化キーと合成したものをパスワードとする。パスワードについては後で詳しく述べる。

【0016】所望とするソフトウェアのパスワードを得たら、暗号を復号する復号プログラムとパスワードからソフトウェアを復元する。まず、CD-ROM2をパーソナルコンピュータ3のCD-ROMドライブ4に挿入し、復号プログラム6をパーソナルコンピュータ3のメモリにロードし起動する。この復号プログラム6はCD-ROM2とは別途にフロッピーディスク等で供給しても、通信回線を通じて送っても、あるいはCD-ROM2へ暗号化せずに格納して供給してもよい。

【0017】次に復号プログラム6は表示装置5へメッセージを出力しパスワードの入力を促し、キーボード8からのパスワードの入力を読み取る。復号プログラム6は読み取ったパスワードから利用者識別情報としての氏名と復号化キーを分離し、復号化キーの正当性を調べ、正当な復号化キーの場合はこの復号化キーでソフトウェアを復号し、復号したソフトウェアの利用者識別情報格納領域へ利用者識別情報である氏名を書き込み、ハードディスク装置(HDD)7へ書き出す。

【0018】ここで、図2および図3を参照してパスワードについて説明する。前にも述べたようにパスワードは暗号を解く復号化キーと利用者識別情報を合成したものである。以下にパスワードの作り方の一例を示す。一例として復号化キーを半角の“xxxx”とし、利用者の氏名を全角の“山田太郎”とすると、xxxxはアスキーコード（十六進数）で78 78 78 78となり、山田太郎はシフトJISコード（同じく十六進数）で8E 52 93 63 91 BE 98 59となる。この2つを氏名の方を初めに交互に1バイト（8ビット）づつ並べ、チェックサムを1バイト最後に加えるたものが図2のa)である。最後のF

(4)

6 はチェックサムで、a) の F6 を除く 2 桁の十六進数をすべて加えあわせて下位の 8 ビットだけをとったものである。b) は a) の十六進数の並びを 2 進数で表記したものの一部である。桁数が長くなるので一部のみを表しているが、この表記は当業者では周知のことなので説明は省略する。

【0019】次に b) の 2 進数を先頭から 6 ビット毎に区切ると c) となり、図 3 の変換表にしたがって文字コードに置き換えパスワードとしたものが f) である。c) から d) への処理は末尾の不足する桁数に 0 (ゼロ) を補ったものであり、d) から e) への処理は 6 ビットの上位桁に 2 桁の 0 (ゼロ) を補って十六進表記にしたものである。このようにして暗号化されたパスワードは、上記と逆の手順で復号化キーと氏名に復元・分離できる。

【0020】なお、以上の例では利用者識別情報として、説明を簡略化するため氏名を使用した。利用者の登録番号(使用許諾を求める時にソフトウェア供給者が付与する管理用の番号)や住所および氏名でもよい。利用者が法人の場合は企業名と所属を格納しておけば企業内での不法コピーも防止できる。また暗号化キーと利用者識別情報を交互に 1 バイトづつ並べて合成したパスワードを作成したが、復号プログラム 6 は個々のソフトウェアの暗号化の情報を持っているので、復号化キーの順序を入れ替えたり、もっと複雑なパスワードにすることも可能である。また、実施例では記憶媒体に CD-ROM を使用したが、CD-ROM に限定する必要はなく、光磁気ディスク、ストリーマ、8 ミリビデオのカセットテープでも良い。

【0021】復号されたソフトウェアは自由にコピーはできるが、ソフトウェアがプログラムの場合は復号されたプログラム自身に利用者識別情報を出力する命令があ

り、またソフトウェアがデータの場合は、データ中に利用者識別情報を含んでいるので、このデータを使用するプログラムは利用者識別情報をデータ中より読みだして出力することができる。

【0022】一例としては、プログラムの実行開始時や初期設定命令を実行している時に、表示装置にソフトウェアのタイトルや開発会社のロゴマークと共に利用者の氏名や登録番号を表示したり、印刷装置にソフトウェアのバージョンと共に印刷することができる。また、パーソナルコンピュータやワークステーションは FM 音源とスピーカを内蔵しているものが多く、利用者の氏名や登録番号を読みあげるようにしてもよい。

【0023】

【発明の効果】以上説明してきたように、この発明によるソフトウェアの配布方法では、パスワードを漏らした漏洩元を容易に特定できるので、ソフトウェアの機密保持およびソフトウェア資産の保護が容易に行える。

【図面の簡単な説明】

【図 1】この発明の一実施例を示すソフトウェアの配布方法を説明する図である。

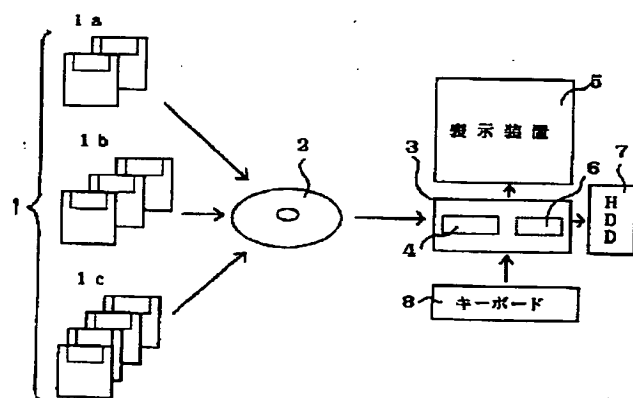
【図 2】この発明に使用するパスワードの合成方法の一例を説明する図である。

【図 3】同じくそのパスワードの作成に用いる変換表の一例を示す図である。

【符号の説明】

- | | |
|---------------|-----------|
| 1 暗号化前のソフトウェア | 2 CD-ROM |
| 3 パーソナルコンピュータ | 4 CD-ROM |
| ドライブ | |
| 5 表示装置 | 6 復号プログラム |
| 7 ハードディスク装置 | 8 キーボード |

【図 1】



【図 2】

- a) 8E 78 52 78 93 78 93 78 91 8E 98 58 F6
↓ 2 進数表記
b) 10001110 01111000 01011001 11110110
↓ 6 ビット毎に区切る
c) 100011 100111 100001 100001 011001 111101 10
↓ 末尾桁数が 6 桁になるように 0 を付加する
d) 100011 100111 100001 100001 011001 111101 100000
↓ それぞれ前に 0 を 2 桁補って 16 進数表記
e) 23 27 21 12 1E 09 00 38 18 37 22 11 2F 29 21 19 3D 20
↓ 図 3 の変換表に従って文字に変換
f) v y v i o j i b l e q n 2 z v r 9 p

(5)

【図3】

00	e	10	H	20	P	30	X
01	f	11	n	21	v	31	3
02	A	12	i	22	Q	32	Y
03	s	13	o	23	v	33	4
04	8	14	J	24	R	34	Z
05	h	15	p	25	x	35	5
06	C	16	k	26	S	36	a
07	i	17	q	27	y	37	6
08	O	18	L	28	T	38	b
09	J	19	r	29	z	39	7
0A	E	1A	M	2A	U	3A	c
0B	K	1B	s	2B	O	3B	8
0C	F	1C	N	2C	V	3C	d
0D	I	1D	t	2D	I	3D	9
0E	G	1E	O	2E	V	3E	e
0F	■	1F	u	2F	2	3F	-

